User Activity on Most Sensitive Computer Systems Is Not Monitored

March 2002

Reference Number: 2002-20-075

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 29, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - User Activity on Most Sensitive Computer Systems Is Not Monitored (Audit # 200120030)

This report presents the results of our review of the Internal Revenue Service's (IRS) efforts to improve its use of activity logs (audit trails) to monitor sensitive computer systems. The IRS uses a system of controls to prevent unauthorized access to sensitive data. Since any system of security controls can be bypassed by experienced hackers or unscrupulous users, audit trails are required to detect unauthorized accesses. Audit trails can alert the IRS that unauthorized accesses have occurred and also provide the evidence needed to investigate and prosecute offenders. We believe the IRS, the nation's largest revenue collector, is a legitimate target for cyber-terrorism and for others wishing to gain access to taxpayers' sensitive financial information. Now, more than ever, a system to detect unauthorized access in the IRS is a necessity.

In the past, we have reported numerous examples of audit trails not being used to monitor IRS mainframe, Unix, and Windows NT operating systems as well as sensitive system applications. The IRS has cited the lack of computer capacity to run and store audit trails, the lack of tools to assist reviewers, the lack of personnel assigned the responsibility to review audit trails, and a lack of guidance on what to review as the reasons it has not monitored user activities. We believe the IRS has not taken adequate actions to overcome these obstacles. In our opinion, many functional executives avoid responsibility for the security of their systems and the data they control, and the Deputy Commissioner for Modernization & Chief Information Officer (CIO) has not placed sufficient emphasis on this issue.

In summary, we found the IRS still does not routinely review audit trails for its sensitive systems except for the Integrated Data Retrieval System (IDRS), the IRS' primary system for accessing taxpayer account information, and possibly a small number of other systems. The IDRS is a major application with a high risk for unauthorized activity. The system provides more than 55,000 users with access to approximately 130 million taxpayer accounts.

An equally significant number of employees have access to the IRS' local area networks and over 250 system applications that contain sensitive data for millions of taxpayer accounts similar to data found on the IDRS. Malicious acts by employees and hackers pose as great a risk for these systems and data as for the IDRS; therefore, it is equally important that the IRS monitor activity on these systems as well.

In our Semiannual Report to the Congress for the period of October 1, 2000, through March 31, 2001, we reported that we identified 163 potential instances where employees browsed taxpayer accounts they were not authorized to access on the IDRS. In contrast, during the past 3 years, only 1 case of potential unauthorized access has been reported to us for all of the other IRS systems, and that case was not identified through an audit trail review. While this is not evidence that security breaches have occurred on those systems, it is a strong indication that unauthorized accesses to taxpayer data on systems other than the IDRS may be occurring without detection.

It is certain that the IRS will not detect such security breaches if it continues to limit effective audit trail reviews to only a few of its hundreds of sensitive computer systems. By not effectively using audit trails to monitor user activity on its computer systems, the IRS enables malicious users to commit security breaches without detection and increases the risk of data tampering, inappropriate access to and disclosure of sensitive taxpayer information, and the disruption of operations.

Over the years, the IRS has generally not considered audit trail requirements in designing and implementing new systems. As a current example, the IRS is undertaking a multi-year business systems modernization project to consolidate its antiquated and widely dispersed mid-range sensitive system applications to platforms at the Computing Centers. As the consolidation progresses and applications are moved to the new platforms, the IRS has not ensured that sufficient capacity exists to run audit trails. In addition, automated audit reporting tools have not been procured to assist in evaluating audit trails, personnel have not been assigned to review audit trails, and guidance on how to review audit trail reports has not been developed.

As a result, the IRS is missing an excellent opportunity to correct the same audit trail security weaknesses identified in the past. Because auditing requirements were not identified and built-in early on, the IRS will not be able to log, monitor, or store records of user activity unless actions are taken.

The Deputy Commissioner for Modernization & CIO should elevate the priority given to establishing an effective audit program to monitor activity on the IRS' sensitive

information systems. Actions taken by management must go beyond past actions that have not effectively corrected these longstanding weaknesses.

We recommend that Information Technology Services (ITS) management and the Office of Security identify and test the resources and system capacity requirements necessary to enable auditing and to log and store operating system activity for all sensitive systems. The CIO should ensure that ITS management obtains and uses automated audit reporting tools for all operating systems. The CIO should also develop a process to ensure that audit trail requirements are identified for all new systems under development**.** The Office of Security and functional managers should identify those individuals responsible for conducting audit trail reviews for all sensitive systems and clearly communicate their responsibilities.

Management's Response: Management's response was due on March 27, 2002. As of March 28, 2002, management had not responded to the draft report.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Scott Wilson, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Background

One of the maxims of security is, "Prevention is ideal, but detection is a must."[1] It is difficult to detect security violations or attacks on a system unless there is a record of system events that can be analyzed. Non-existent or incomplete logging of operating system and network device activity is considered 1 of the 10 most critical Internet security vulnerabilities.[2] If a system is attacked, without an audit trail review there is little chance of discovering what the attacker did. System administrators and users inside an organization are more likely to engage in malicious activities and make errors if they know their activity is not recorded or monitored. In addition, recovery from system failures may be more difficult when events are not recorded.

The Department of the Treasury requires that automated information systems and networks which process, store, or transmit Sensitive But Unclassified information maintain an audit trail of user security relevant events and ensure that this security feature is properly implemented and protected from modification. The National Institute of Standards and Technology and the General Accounting Office provide guidelines for agencies to comply with federal information systems security requirements.

Internal Revenue Service (IRS) managers and the Treasury Inspector General for Tax Administration's (TIGTA) Office of Investigations have responsibilities for analyzing audit trail data. IRS managers have overall responsibility for the security of their systems and should review audit trails to detect inappropriate and malicious activities. The Office of Investigations relies on these audit trails to investigate suspicious activities and to detect unauthorized accesses to taxpayer data by employees.

The IRS has effective audit procedures in place to ensure that audit trail reports for the Integrated Data Retrieval

[1] Security Administrators, Networking and Security (SANS) Institute/Federal Bureau of Investigation (FBI), The Twenty Most Critical Internet Security Vulnerabilities, October 1, 2001.

[2] SANS/FBI, The Twenty Most Critical Internet Security Vulnerabilities, October 1, 2001.

system (IDRS)[3] are regularly reviewed to deter and detect unauthorized access or misuse of taxpayer data and accounts. IDRS audit trail reviews have consistently identified potential unauthorized access to taxpayer accounts in spite of the IRS' zero tolerance policy and awareness programs. In its Semiannual Report to the Congress for the period of October 1, 2000, through March 31, 2001, the TIGTA reported that it identified 163 potential IDRS security breaches that were referred to its field staff for further investigation. In contrast, during the past 3 years, only 1 case of potential unauthorized access has been reported to the TIGTA for all of the other IRS systems, and that case was not identified through an audit trail review.

The consistent identification of IDRS security breaches is a strong indication that unauthorized accesses to taxpayer data may be occurring without detection on other systems that provide access to the same type of sensitive taxpayer data as the IDRS. It is certain that the IRS and the TIGTA Office of Investigations will not detect such security breaches if the IRS continues to generate audit trails on only a few of its hundreds of sensitive computer systems.

The TIGTA's Office of Audit and the IRS' Office of Security reviews have identified the following as pervasive causes for the lack of an effective auditing program for all sensitive systems:

- Enabling auditing adversely affects system performance.
- The IRS lacks automated audit reporting tools.
- Guidelines to assist in conducting audit trail reviews are not sufficient.
- Audit trail review responsibilities are not assigned.

We evaluated the IRS' efforts to resolve these issues and found that, while progress has been made, these issues continue to be an obstacle to realizing an effective auditing

[3] The IDRS is the IRS' main database of taxpayer accounts. It is used by IRS personnel to research and update taxpayer account data.

program for the mainframe, Unix, and Windows NT sensitive systems. While we recognize that the review of audit trails for an organization that has as many sensitive systems as the IRS is difficult and costly, the risks of intrusions by hackers and unauthorized accesses by employees necessitate a consistent and comprehensive effort.

In our opinion, the IRS' functional managers have avoided their responsibility to detect security breaches of their systems, and the Deputy Commissioner for Modernization & Chief Information Officer (CIO) has not devoted sufficient efforts in ensuring that unauthorized accesses are identified. By not effectively using audit trails to monitor user activity on its computer systems, the IRS enables malicious users to commit security breaches without detection and increases the risk of data tampering, inappropriate access to and disclosure of sensitive taxpayer information, and the disruption of operations.

We conducted this audit in the Information Technology Services (ITS) Headquarters office and the Small Business/Self-Employed Headquarters office between March and October 2001. We interviewed key personnel and reviewed relevant documentation. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Audit Trail Controls Are Routinely Disabled

Management has routinely disabled audit trails citing the lack of computer capacity. As a result, unauthorized accesses by employees and hackers may have gone undetected. For example, audit trails were turned off on the Collection system used to track lien assignments and lien due dates, the Examination system used to assign returns for audit and update taxpayer accounts, and the Criminal Investigation system used to identify fraud on electronically filed returns. In addition, a recent TIGTA audit[4] of a mainframe system found that the system level auditing

[4] *Controls Over the IRS' Masterfile System Are Generally Adequate, But Some Improvement Is Needed*, (Reference Number 2001-20-092, dated June 2001).

facility was routinely postponed during workload peaks to allow users to perform their assigned responsibilities.

Although the lack of computer capacity to run and store audit trails is routinely cited, we know of no formal studies conducted to test the impact of audit trails on computer performance. Nor are we aware of any attempts by management to reduce the impact on computer performance by limiting the amount of data captured.

All systems processing or storing sensitive information must have an audit logging capability. IRS guidelines further state that it is not enough for an operating system to contain all of the relevant security features; those features must be enabled. The Federal Information Processing Standards (FIPS) and other relevant federal guidelines state that selecting the specific data to be captured and logged is a managerial decision that should be made only after detailed analysis by both users and data processing personnel. The system must be able to easily off-load voluminous journal data, to condense it as much as possible, and to easily on-load the same data for later inspection.

Recommendations

1. The Office of Security should continue to work with business unit managers and the TIGTA Office of Investigations to conduct risk assessments of specific systems and locations. The assessment should be used to determine the minimum audit trail information needed to detect unauthorized accesses. The Systems Support Division should test the impact of the auditing requirements on system capacity. Depending on the test results and identification of required resources, the Office of Security, ITS, and business unit managers should coordinate to balance audit trail requirements with system capacity needs. The Systems Support Division should then identify capacity requirements and procure the hardware necessary to enable auditing.

Management's Response: Management's response was due on March 27, 2002. As of March 28, 2002, management had not responded to the draft report.

2. The Deputy Commissioner for Modernization & CIO should identify and address system capacity shortfalls to ensure that mainframe, Unix, and Windows NT system activity will be logged and stored.

The Internal Revenue Service Lacks Automated Audit Reporting Tools

Nationwide, user activity for mainframe, Unix, and Windows NT operating systems and some sensitive system applications continues to go unmonitored due to the lack of automated reporting tools to help dissect the voluminous audit trail data. Audit trail data that is too voluminous cannot be effectively reviewed increasing the risk that unauthorized user access or activity will not be detected.

The FIPS state that audit reports and other output must be as concise as possible and specifically pinpoint any unusual activity. Long reports containing large amounts of data may actually decrease detection of security violations. Audit reporting tools should be used to produce readable and manageable audit trail reports from the voluminous security event logs. Audit report tools should also be used to analyze the voluminous audit log data to assist in identifying trends that indicate potential security breaches. Such automated tools have been implemented to effectively accomplish IDRS audit trail reviews and are the reason for the consistent identification of unauthorized accesses on that system.

The Office of Security has determined that the lack of automated reporting tools is a weakness for all operating systems including some mainframe systems. It recently made progress regarding automated reporting tools for the Windows NT and Unix operating systems. The IRS has procured a commercial off-the-shelf product to create readable reports from the voluminous data in the NT system audit logs. The software can also assist in identifying trends that may indicate potential security breaches. The Office of Security has also been researching a similar automated reporting tool for the IRS' Unix operating systems. Procuring these tools will move the IRS much closer to being able to meet its Unix and Windows NT auditing requirements.

Recommendation

3. The Deputy Commissioner for Modernization & CIO should ensure that ITS management obtains and uses automated audit reporting tools for the Unix and Windows NT operating systems. The availability of audit reporting tools for mainframe systems should also be explored.

Guidelines to Assist in Conducting Audit Trail Reviews Are Not Sufficient

Audit trail data for the mainframe, Unix, and Windows NT operating systems as well as some sensitive system applications were not reviewed, in part, because national guidelines were not available to assist security personnel in how to conduct the audit trail reviews. Without review guidelines, personnel responsible for reviewing audit trail reports will not recognize normal vs. abnormal events to effectively detect unusual activity.

The Office of Security's response to a previous TIGTA report included a corrective action to improve Windows NT guidelines.[5] It committed to establishing the National Taskforce Security Evaluation Committee (NTSEC) to develop policies and procedures to review mainframe, Unix, and Windows NT operating system audit trails. Policies and procedures training was intended to accompany the implementation. These actions were scheduled for completion by July 1, 2001.

Due to other priorities, neither this date nor a second proposed completion date of October 2001 for an NTSEC group charter were met. As of the date of this report, the Office of Security had a signed charter, dated November 2001, and was attempting to recruit members of the committee that will develop policies and procedures for conducting the audit trail reviews.

Guidelines to assist in reviewing audit trails of most sensitive system applications are also insufficient or do not exist. An exception to this is the Midwest Automated Compliance System (MACS). The IRS has developed audit

[5] *Computer Security Controls Should Be Strengthened in the Former Northern California District*, (Reference Number 2001-20-036, dated January 2001).

trail review guidelines for the MACS. The system provides access to facsimiles of taxpayer returns for use in return examination activities. The MACS audit trail review guidelines provide assistance to the reviewers in how to analyze the audit trail reports to identify the types of security breaches that may occur on that system. The review includes comparing activity to source documents to ensure that system accesses are authorized.

Review guidelines have not been developed for most sensitive systems, however. For example, review guidelines were not developed for the Collection system used to track liens and the Examination system used to track and update audits. In response to a prior audit report, audit trail training for the lien system was to be completed by September 2001 but has not yet been given. Audit trail guidelines for the Examination system have not been developed due to other priorities. Based on prior audit work, we believe the conditions reported for these systems are indicative of most other sensitive systems in the IRS.

Recommendations

4. The Office of Security, in conjunction with ITS and business unit managers, should develop guidelines for use in conducting mainframe, Unix, and Windows NT operating system audit trail reviews, including procedures to ensure the required reviews are conducted and documented. The TIGTA Office of Investigations should be consulted to ensure that procedures are adequate for investigative purposes.
5. The Office of Security should work with business unit managers to develop auditing guidelines for all sensitive system applications that do not already have them. The audit trail review requirements included in these guidelines should be based on risk.

Audit Trail Review Responsibilities Are Not Assigned

The IRS has not assigned sufficient staffing to review audit trails. Even if the IRS had the computer capacity, tools, and guidelines to review audit trails, potential attacks could go unnoticed unless staff is available to review them. Responsibility for conducting audit trails has not been

clearly assigned to either the CIO's security specialists or to the business units.

National Institute for Standards and Technology (NIST) guidelines for implementing effective security programs state that computer security responsibilities and accountabilities should be made explicit. The IRS' Functional Audit Requirements for Implementation in IRS Computing Systems recognizes that there cannot be an audit program without personnel available to review reports.

The Office of Security has initiated an agency-wide effort to improve the identification and assignment of security roles and responsibilities for all sensitive systems. Until this is accomplished, the IRS will not have personnel in place to effectively monitor user activity to detect any unauthorized activity that may be occurring on its systems.

Recommendation

6. The Office of Security should coordinate with business unit managers to identify those individuals responsible for conducting audit trail reviews for all sensitive systems.

Common Audit Trail Review Issues Will Continue With the Tier II Consolidation Project

The IRS is undertaking a multi-year Tier II[6] Consolidation Project to improve management of its mid-level computer systems. The project will result in consolidating most of the over 250 Tier II applications from many antiquated servers across the country to platforms at the computing centers. This will result in a standardized Unix operating environment and cost savings. The Tier II Consolidation Project presents an opportunity to address and correct the persistent audit trail issues that have long prevented the use of audit trails to monitor Unix operating system activity.

ITS management has not taken advantage of this opportunity. Auditing requirements were not adequately considered during the design and testing of this project. The System Support Division of ITS stated that the consolidation platforms lack the capacity to record and store

[6] Tier II systems are all multi-user systems that are neither Tier I mainframe systems nor Tier III stand-alone PCs/Workstations.

the system activity as set forth in the functional audit requirements. At the time of our fieldwork, it had not communicated this to the Office of Security, nor had it conducted any tests to measure the impact of the requirements on system performance and resource requirements.

In addition, an automated reporting tool had not been procured and implemented, guidelines for how to review audit trail reports had not been developed, and responsibility for conducting audit trail reviews had not been assigned. As a result, the consolidation will not result in improved accountability for user actions. System events and activity will continue to go unmonitored because the modernized, consolidated system will carry with it the same audit trail security weaknesses as the antiquated servers it is replacing.

Recommendations

7. The Deputy Commissioner for Modernization & CIO should emphasize the need for logging, storing, and reviewing sufficient audit trail information during the systems development and certification and accreditation processes for all new systems.
8. The Chief, ITS, in conjunction with the Director, Office of Security, should ensure that all recommendations in this report to improve system capacity, use audit reporting tools, develop audit trail review guidelines, and assign audit trail review responsibility are applied to the Tier II consolidation.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate Internal Revenue Service (IRS) efforts to improve its use of activity logs (audit trails) to monitor sensitive computer systems. We conducted this audit to assess the IRS' initiatives in response to its long-standing need to improve the review of user activity on its sensitive operating systems and applications. To accomplish our objective, we:

I. Identified requirements, standards, procedures, and guidelines designed to ensure that systems are monitored to detect unauthorized access. Reviewed the following sources:

   A. National Institute of Standards and Technology (NIST) Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook.*

   B. NIST Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems.*

   C. NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems.*

   D. OMB Circular No. A-130, *Security of Federal Automated Information Resources, Appendix III* (minimum set of controls to be included in Federal automated information security programs).

   E. Department of the Treasury Security Manual.

II. Identified and analyzed all Treasury Inspector General for Tax Administration (TIGTA), General Accounting Office (GAO), and IRS reviews from the past 2 years that reported audit trail control weaknesses.

   A. Categorized all of the audit trail issues by type, e.g., capacity, lack of training, etc.

   B. Documented IRS corrective actions taken or proposed for each issue.

   C. Determined if IRS corrective actions to TIGTA and GAO findings adequately address the root cause of the audit trail control weaknesses.

III. Determined how the IRS ensures that it is in compliance with requirements that an audit mechanism be in place to record, examine, and review any or all security-related system activities.

   A. Interviewed Office of Security personnel to determine if the IRS has a method in place to collectively address the status of audit trail requirements for all of its TIER II systems (similar to standardized Windows NT requirements) and to identify systems not in compliance.

B. Determined if the IRS considers system capacity needs during the design phase of its sensitive systems to ensure that all necessary hardware and software requirements are in place to produce audit trails.

C. Determined if the IRS ensures that for each of its sensitive systems there are adequate guidelines and training, assignment of responsibility for audit trail review, and methods to ensure that reviews are performed.

D. Determined if IRS management is aware of the extent to which any audit trail capability for its sensitive systems is currently disabled.

E. Determined if the IRS ensures audit trail data are sufficient, manageable (volume), and readable. Determined if management has:

- Carefully selected the activities to be logged for each sensitive system.
- Used audit reduction, trend/variance-detection, or attack signature-detection tools to assist in the audit trail review, when necessary.

F. Reviewed system certification documents for the Automated Lien System and the Examination Returns Control System to determine if the Trusted Facility Manual, Security Plan, and Security Features Users Guide adequately address audit trail requirements, guidance, and procedures.

IV. Determined if the IRS places sufficient emphasis on monitoring access to its sensitive systems, similar to its emphasis on access to the Integrated Data Retrieval System (IDRS).[1]

A. Contacted the TIGTA Office of Investigations to identify the number and results of any unauthorized access cases (other than to the IDRS) investigated over the past 2-year period.

B. Determined if the IRS tracks unauthorized access to other sensitive systems as it does for the IDRS.

[1] The IDRS is the IRS' main database of taxpayer accounts. It is used by IRS personnel to research and update taxpayer account data.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Gerald Horn, Audit Manager
Joan Raniolo, Senior Auditor
Charles Ekholm, Auditor
David Hodge, Auditor
William Simmons, Auditor

Appendix III

Report Distribution List

Commissioner N:C
Deputy Commissioner N:DC
Chief, Information Technology Services M:I
Director, Office of Security M:S
Chief Counsel CC
National Taxpayer Advocate TA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Office of Management Controls N:CFO:F:M
Audit Liaison: Deputy Commissioner for Modernization & Chief Information Officer M